(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2012 년 7 월 26 일 (26.07.2012)

WIPO | PCT

(10) 국제공개번호
WO 2012/099330 A2

(51) 국제특허분류:
H04W 12/06 (2009.01) *H04L 9/32* (2006.01)

(21) 국제출원번호: PCT/KR2011/009196

(22) 국제출원일: 2011 년 11 월 30 일 (30.11.2011)

(25) 출원언어: 한국어

(26) 공개언어: 한국어

(30) 우선권정보:
10-2011-0005787 2011 년 1 월 20 일 (20.01.2011) KR

(71) 출원인 (US 을(를) 제외한 모든 지정국에 대하여): **에스케이플래닛 주식회사 (SK PLANET CO., LTD.)** [KR/KR]; 서울시 중구 을지로 2 가 11 번지, 100-999 Seoul (KR).

(72) 발명자; 겸
(75) 발명자/출원인 (US 에 한하여): **이정훈 (LEE, Jeong Hoon)** [KR/KR]; 서울시 서초구 잠원동 녹원한신아파트 102 동 1503 호, 137-030 Seoul (KR). **허훈 (HUH, Hun)** [KR/KR]; 경기도 용인시 수지구 동천동 신명스카이뷰 504 동 205 호, 448-120 Gyeonggi-do (KR). **이은복 (LEE, Eun Bok)** [KR/KR]; 서울시 송파구 잠실 3 동 레이크팰리스아파트 134 동 1301 호, 138-223 Seoul (KR).

(74) 대리인: **특허법인 화우 (YOON & YANG)**; 서울시 강남구 대치동 997-9 삼호빌딩 4 층, 135-502 Seoul (KR).

(81) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 국내 권리의 보호를 위하여): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

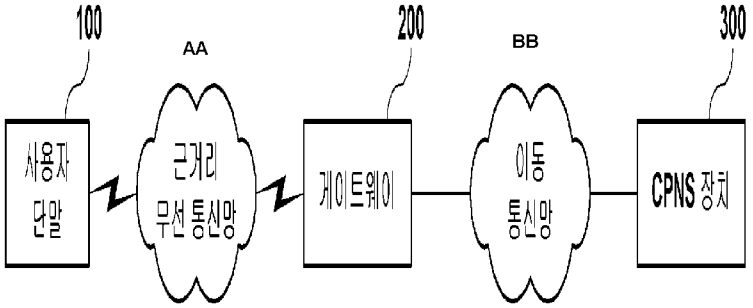
(84) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 역내 권리의 보호를 위하여): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), 유라시아 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), 유럽 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR),

[다음 쪽 계속]

(54) **Title**: SYSTEM AND METHOD FOR ISSUING AN AUTHENTICATION KEY FOR AUTHENTICATING A USER IN A CPNS ENVIRONMENT

(54) **발명의 명칭** : C P N S 환경에서 사용자 인증을 위한 인증키 발급 시스템 및 방법

[Fig. 1]



100 ... User terminal
200 ... Gateway
300 ... CPNS device
AA ... Near field communication network
BB ... Mobile communication network

(57) **Abstract**: The present invention relates to a system and method for issuing an authentication key for authenticating a user in a CPNS environment, which involve: a user terminal which has a near field communication function for requesting that a gateway registers terminal information including an ID and passcode, and when the ID and passcode for using a CPNS service are inputted, encrypts the terminal information including the ID and passcode using the passcode, transmits an authentication request signal including the encrypted terminal information to the gateway, and receives an authentication key generated by a CPNS device; said gateway which has a mobile communication or near field communication function for transmitting the terminal information to the CPNS device via a mobile communication network in response to the request for terminal information registration from the user terminal, and when the authentication request signal is received from the user terminal, transmits the encrypted terminal information to the CPNS device to request authentication; and the CPNS device which receives the terminal information from the gateway to store the terminal information, decrypts the encrypted terminal information in response to the authentication request from the gateway to perform user authentication, generates the authentication key for the CPNS service when a user is authenticated, and encrypts the generated authentication key using the passcode so as to provide the authentication

[다음 쪽 계속]

WO 2012/099330 A2

OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

공개:

— 국제조사보고서 없이 공개하며 보고서 접수 후 이를 별도 공개함 (규칙 48.2(g))

key to the user terminal via the gateway. Therefore, according to the present invention, when one user uses several terminals in the CPNS environment, the terminals can be easily authenticated, and keys for the security of the terminals can be conveniently managed.

(57) 요약서: 본 발명은 CPNS 환경에서 사용자 인증을 위한 인증키 발급 시스템 및 방법에 관한 것으로서, 근거리 무선 통신 기능이 탑재되어, 아이디 및 비밀번호를 포함하는 단말정보의 등록을 게이트웨이에 요청하고, CPNS 서비스 이용을 위한 아이디 및 비밀번호가 입력된 경우, 상기 아이디와 비밀번호를 포함하는 단말정보를 상기 비밀번호를 이용하여 암호화하고, 상기 암호화된 단말정보를 포함하는 인증 요청 신호를 상기 게이트웨이에 전송하여 CPNS 장치에서 생성된 인증키를 수신하는 사용자 단말, 이동 통신 기능 또는 근거리 무선 통신 기능을 탑재하여, 상기 사용자 단말로부터의 단말정보 등록 요청에 따라 상기 단말정보를 이동통신망을 통해 CPNS 장치에 전송하고, 상기 사용자 단말로부터 인증 요청 신호가 수신된 경우 상기 암호화된 단말정보를 상기 CPNS 장치에 전송하여 인증을 요청하는 게이트웨이, 상기 게이트웨이로부터 단말정보를 수신하여 저장하고, 상기 게이트웨이로부터의 인증 요청에 따라 상기 암호화된 단말정보를 해독하여 사용자 인증을 수행하고, 인증된 경우 CPNS 서비스를 위한 인증키를 생성하고, 상기 생성된 인증키를 상기 비밀번호를 이용하여 암호화하여 상기 게이트웨이를 통해 상기 사용자 단말에 제공하는 CPNS 장치를 포함한다. 따라서, 본 발명에 따르면, CPNS 환경에서 한 사용자가 여러 개의 단말을 사용할 경우, 이를 손쉽게 인증할 수 있고, 각 단말별로 보안을 확보하기 위한 편리한 키 관리 방법을 제공할 수 있다.

명세서

발명의 명칭: C P N S 환경에서 사용자 인증을 위한 인증키 발급 시스템 및 방법

기술분야

[1] 본 발명은 CPNS(Converged Personal Network Service) 환경에서 사용자 인증을 위한 인증키 발급 시스템 및 방법에 관한 것으로, 더욱 상세하게는 근거리 무선 통신 기능이 탑재된 사용자 단말이 CPNS 서비스 이용을 위한 아이디 및 비밀번호를 입력받은 경우, 상기 아이디와 비밀번호를 포함하는 단말정보를 상기 비밀번호를 이용하여 암호화하고, 상기 암호화된 단말정보를 포함하는 인증 요청 신호를 상기 게이트웨이에 전송하여 CPNS 장치에서 생성된 인증키를 수신하고, CPNS 장치가 상기 게이트웨이로부터의 인증 요청에 따라 상기 암호화된 단말정보를 해독하여 사용자 인증을 수행하고, 인증된 경우 CPNS 서비스를 위한 인증키를 생성 및 상기 비밀번호를 이용하여 암호화하여 상기 게이트웨이를 통해 상기 사용자 단말에 제공하는 CPNS 환경에서 사용자 인증을 위한 인증키 발급 시스템 및 방법에 관한 것이다.

배경기술

[2] CPNS(Converged Personal Network Service) 환경이란, 근거리 무선 통신만 가능할 뿐, 이동 통신망과의 Cellular 통신이 불가능한 사용자 단말이 PN(Personal Network Service) 게이트웨이 역할을 수행하는 이동통신 단말과 근거리 무선 통신을 수행하여, Cellular 통신을 통해 제공받을 수 있는 데이터 서비스를 이용할 수 있도록 하는 것이다.

[3] 근거리 무선 통신만 가능할 뿐, 이동 통신망과의 Cellular 통신이 불가능한 사용자 단말이 CPNS 서비스를 이용하기 위해서는 초기 설정 과정을 거치게 된다.

[4] 즉, 상기 사용자 단말은 CPNS 서비스를 이용하기 위하여, PN(Personal Network) Gateway Device 역할을 수행할 게이트웨이를 검색한다. 이후, 상기 게이트웨이는 상기 사용자 단말로부터의 단말 정보를 이용하여 상기 사용자 단말의 CPNS 서비스 가능 여부를 체크한다. 상기 체크 결과 CPNS 서비스가 가능할 경우, 상기 게이트웨이는 상기 사용자 단말로 CPNS 서비스가 가능하다는 인증 메시지를 전송한다.

[5] 상기와 같은 초기 설정 과정을 거쳐야 상기 사용자 단말은 데이터 서비스를 이용할 수 있게 된다.

[6] 그러나 상기와 같은 종래의 방법은 CPNS 환경에서 한 사용자가 여러 개의 단말을 사용할 경우에는 각 단말에 대해 별도의 인증과정을 거쳐야 하는 번거로운 단점이 있다.

발명의 상세한 설명

기술적 과제

[7] 본 발명은 상기한 문제점을 해결하기 위하여 안출한 것으로, 본 발명의 목적은 CPNS 환경에서 한 사용자가 여러 개의 단말을 사용할 경우, 이를 손쉽게 인증할 수 있고, 각 단말별로 보안을 확보하기 위한 편리한 키 관리 방법을 제공할 수 있는 CPNS 환경에서 사용자 인증을 위한 인증키 발급 시스템 및 방법을 제공하는데 있다.

[8] 본 발명의 다른 목적은 USIM의 Credential과 같이 미리 할당된 인증키가 아니더라도, 사용자가 스스로 정한 비밀번호(Password)를 사용하여 Credential과 같은 결과를 얻을 수 있는 CPNS 환경에서 사용자 인증을 위한 인증키 발급 시스템 및 방법을 제공하는데 있다.

과제 해결 수단

[9] 상기 목적들을 달성하기 위하여 본 발명의 일 측면에 따르면, 근거리 무선 통신 기능이 탑재되어, 아이디(ID) 및 비밀번호를 포함하는 단말정보의 등록을 게이트웨이에 요청하고, CPNS(Converged Personal Network Service) 서비스 이용을 위한 아이디 및 비밀번호가 입력된 경우, 상기 아이디 및 비밀번호를 포함하는 단말정보를 상기 비밀번호를 이용하여 암호화하고, 상기 암호화된 단말정보를 포함하는 인증 요청 신호를 상기 게이트웨이에 전송하여 CPNS 장치에서 생성된 인증키를 수신하는 사용자 단말, 이동 통신 기능 또는 근거리 무선 통신 기능을 탑재하여, 상기 사용자 단말로부터의 단말정보 등록 요청에 따라 상기 단말정보를 이동통신망을 통해 CPNS 장치에 전송하고, 상기 사용자 단말로부터 인증 요청 신호가 수신된 경우 상기 암호화된 단말정보를 상기 CPNS 장치에 전송하여 인증을 요청하는 게이트웨이, 상기 게이트웨이로부터의 단말정보를 저장하고, 상기 게이트웨이로부터의 인증 요청에 따라 상기 암호화된 단말정보를 해독하여 사용자 인증을 수행하고, 인증된 경우 CPNS 서비스를 위한 인증키를 생성하고, 상기 생성된 인증키를 상기 비밀번호를 이용하여 암호화한 후, 상기 게이트웨이를 통해 상기 사용자 단말에 제공하는 CPNS 장치를 포함하는 CPNS 환경에서 사용자 인증을 위한 인증키 발급 시스템이 제공된다.

[10] 상기 게이트웨이는 상기 사용자 단말로부터의 단말정보 등록 요청에 따라 상기 단말정보를 저장하고, 상기 사용자 단말로부터 인증 요청 신호가 수신된 경우 상기 암호화된 단말정보를 해독하여 사용자 인증을 수행하고, 인증된 경우 CPNS 서비스를 위한 인증키를 생성하고, 상기 생성된 인증키를 상기 비밀번호를 이용하여 암호화한 후 상기 사용자 단말 및 CPNS 장치에 제공할 수 있다.

[11] 본 발명의 다른 측면에 따르면, 통신망을 통해 정보를 송수신하기 위한 통신 인터페이스부, 사용자 명령을 입력받는 입력부, 상기 입력부를 통해 CPNS 서비스 이용을 위한 아이디 및 비밀번호가 입력된 경우, 상기 아이디 및

비밀번호를 포함하는 단말정보를 상기 비밀번호를 이용하여 암호화하는 암호화부, 상기 암호화된 단말정보를 포함하는 인증 요청 신호를 상기 통신 인터페이스부를 통해 게이트웨이에 전송하는 인증 요청부, 상기 인증 요청에 따라 CPNS 장치에서 생성된 인증키를 상기 게이트웨이로부터 수신 및 저장하는 인증키 관리부를 포함하는 사용자 단말이 제공된다.

[12] 상기 사용자 단말은 상기 입력부를 통해 입력된 아이디 및 비밀번호를 포함하는 단말정보를 근거리 무선 통신망을 통해 상기 게이트웨이에 전송하여 상기 CPNS 장치에 등록 요청하는 단말 정보 등록 요청부를 더 포함할 수 있다.

[13] 상기 단말 정보 등록 요청부는 상기 아이디 및 비밀번호를 포함하는 단말정보를 상기 비밀번호를 이용하여 암호화하고, 상기 암호화된 단말정보를 근거리 무선 통신망을 통해 상기 게이트웨이에 전송하여 상기 CPNS 장치에 등록 요청한다.

[14] 또한, 상기 사용자 단말은 상기 인증키를 이용하여 CPNS 서비스를 실행하는 서비스 실행부를 더 포함할 수 있다.

[15] 또한, 상기 사용자 단말은 상기 입력부를 통해 CPNS 서비스 이용을 위한 아이디 및 비밀번호가 입력된 경우, 상기 아이디와 비밀번호를 저장함과 동시에 인증키를 생성하는 인증키 생성부, 상기 아이디 및 비밀번호를 포함하는 단말정보와 상기 생성된 인증키를 상기 비밀번호를 이용하여 암호화하여 CPNS 장치로 전송하는 인증키 제공부를 더 포함할 수 있다.

[16] 본 발명의 또 다른 측면에 따르면, 통신망을 통해 정보를 송수신하기 위한 통신 인터페이스부, 사용자 단말별 아이디 및 비밀번호를 포함하는 단말정보, 인증키가 저장된 단말 정보 데이터베이스, 상기 통신 인터페이스부를 통해 단말정보의 등록이 요청된 경우, 상기 단말정보를 상기 단말정보 데이터베이스에 등록하는 단말정보 등록부, 상기 통신 인터페이스부를 통해 인증 요청 신호가 수신된 경우, 상기 인증 요청 신호에 포함된 단말정보를 해독하고, 상기 해독된 단말정보가 상기 단말정보 데이터베이스에 존재하는지의 여부를 이용하여 사용자 인증을 수행하는 인증부, 상기 사용자가 인증된 경우, CPNS 서비스를 위한 인증키를 생성하는 인증키 생성부, 상기 생성된 인증키를 상기 단말정보에 포함된 비밀번호를 이용하여 암호화하고, 상기 암호화된 인증키를 상기 통신 인터페이스부를 통해 해당 사용자 단말에 제공하는 인증키 제공부를 포함하는 CPNS 장치가 제공된다.

[17] 상기 단말정보는 아이디, 비밀번호, 단말 고유번호, 단말 종류, 단말 기종 중 적어도 하나를 포함할 수 있다.

[18] 본 발명의 또 다른 측면에 따르면, (a) 사용자 단말이 상기 암호화된 단말정보를 포함하는 인증 요청 신호를 근거리 무선 통신망을 통해 게이트웨이에 전송하는 단계, (b) 상기 게이트웨이가 상기 인증 요청 신호내 암호화된 단말정보를 저장함과 동시에 이동통신망을 통해 CPNS 장치에 전송하여 인증을 요청하는 단계, (c) 상기 CPNS 장치가 상기 게이트웨이로부터의 인증 요청에 따라 상기

암호화된 단말정보를 해독하여 사용자 인증을 수행하는 단계, (d) 상기 사용자가 인증된 경우, 상기 CPNS 장치가 CPNS 서비스를 위한 인증키를 생성하는 단계, (e) 상기 CPNS 장치가 상기 생성된 인증키를 상기 비밀번호를 이용하여 암호화하고, 상기 암호화된 인증키를 상기 게이트웨이를 통해 상기 사용자 단말에 제공하는 단계를 포함하는 CPNS 환경에서 사용자 인증을 위한 인증키 발급 방법이 제공된다.

[19] 본 발명의 또 다른 측면에 따르면, 사용자 단말이 CPNS 환경에서 사용자 인증을 위한 인증키를 발급받기 위한 방법에 있어서, (a) 사용자에 의해 CPNS 서비스 이용을 위한 아이디 및 비밀번호가 입력된 경우, 상기 아이디와 비밀번호를 포함하는 단말정보를 상기 비밀번호를 이용하여 암호화하는 단계, (b) 상기 암호화된 단말정보를 포함하는 인증 요청 신호를 게이트웨이에 전송하는 단계, (c) 상기 인증 요청에 따라 CPNS 장치에서 생성된 인증키를 상기 게이트웨이로부터 수신 및 저장하는 단계, (d) 상기 인증키를 통해 상기 CPNS 장치에 접속되어 CPNS 서비스를 실행하는 단계를 포함하는 CPNS 환경에서 사용자 인증을 위한 인증키 발급 방법이 제공된다.

[20] 상기 CPNS 환경에서 사용자 인증을 위한 인증키 발급 방법은 상기 (a) 단계 이전에 상기 사용자에 의해 입력된 아이디 및 비밀번호를 포함하는 단말정보의 등록을 상기 게이트웨이에 요청하는 단계를 더 포함할 수 있다.

[21] 본 발명의 또 다른 측면에 따르면, CPNS 장치가 CPNS 환경에서 사용자 인증을 위한 인증키를 발급하는 방법에 있어서, (a) 게이트웨이로부터 CPNS 서비스 이용을 위한 인증 요청 신호가 수신된 경우, 상기 인증 요청 신호에 포함된 암호화된 단말정보를 해독하는 단계, (b) 상기 해독된 단말정보가 기 저장된 단말정보 데이터베이스에 존재하는지의 여부를 판단하는 단계, (c) 상기 단말정보가 상기 단말정보 데이터베이스에 존재하는 경우, CPNS 서비스를 위한 인증키를 생성하는 단계, (d) 상기 생성된 인증키를 상기 단말정보에 포함된 비밀번호를 이용하여 암호화하는 단계, (e) 상기 암호화된 인증키를 상기 게이트웨이를 통해 해당 사용자 단말에 제공하는 단계를 포함하는 CPNS 환경에서 사용자 인증을 위한 인증키 발급 방법이 제공된다.

[22] 상기 CPNS 환경에서 사용자 인증을 위한 인증키 발급 방법은 상기 (a) 단계 이전에 상기 게이트웨이로부터 아이디 및 비밀번호를 포함하는 단말정보의 등록이 요청된 경우, 상기 단말정보를 등록하는 단계를 더 포함할 수 있다.

발명의 효과

[23] 상술한 바와 같이 본 발명에 따르면, CPNS 환경에서 한 사용자가 여러 개의 단말을 사용할 경우, 이를 손쉽게 인증할 수 있고, 각 단말별로 보안을 확보하기 위한 편리한 키 관리 방법을 제공할 수 있다.

[24] 또한, 비밀번호는 사용자가 손쉽게 기억하고 항상 비밀을 유지하는바, 사용자 단말을 이용하여 CPNS 서비스를 이용하기 위한 초기 인증키 할당 방법을

단순화할 수 있다.

도면의 간단한 설명

[25] 도 1은 본 발명의 일 실시예에 따른 CPNS 환경에서 사용자 인증을 위한 인증키 발급 시스템을 나타낸 도면.

[26] 도 2는 도 1에 도시된 사용자 단말의 구성을 개략적으로 나타낸 블럭도.

[27] 도 3은 도 1에 도시된 CPNS 장치의 구성을 개략적으로 나타낸 블럭도.

[28] 도 4는 본 발명의 일 실시예에 따른 CPNS 환경에서 사용자 인증을 위한 인증키 발급 방법을 나타낸 도면.

[29] 도 5는 본 발명의 다른 실시예에 따른 CPNS 환경에서 사용자 인증을 위한 인증키 발급 시스템을 나타낸 도면.

[30] 도 6은 도 5에 도시된 게이트웨이의 구성을 개략적으로 나타낸 블럭도.

[31] 도 7은 본 발명의 다른 실시예에 따른 CPNS 환경에서 사용자 인증을 위한 인증키 발급 방법을 나타낸 도면.

[32] 도 8은 본 발명의 또 다른 실시예에 따른 CPNS 환경에서 사용자 인증을 위한 인증키 발급이 가능한 사용자 단말의 구성을 개략적으로 나타낸 블럭도.

[33] 도 9는 도 8에 도시된 사용자 단말이 CPNS 환경에서 사용자 인증을 위한 인증키를 발급하는 방법을 나타낸 흐름도.

발명의 실시를 위한 형태

[34] 본 발명의 전술한 목적과 기술적 구성 및 그에 따른 작용 효과에 관한 자세한 사항은 본 발명의 명세서에 첨부된 도면에 의거한 이하 상세한 설명에 의해 보다 명확하게 이해될 것이다.

[35] 도 1은 본 발명의 일 실시예에 따른 CPNS 환경에서 사용자 인증을 위한 인증키 발급 시스템을 나타낸 도면이다.

[36] 도 1을 참조하면, CPNS 환경에서 사용자 인증을 위한 인증키 발급 시스템은 근거리 무선 통신 기능이 탑재된 사용자 단말(100), 이동통신 기능 및 근거리 무선 통신 기능이 탑재되어 상기 사용자 단말(100)과 CPNS 장치(300)와의 인터페이스를 제공하는 게이트웨이(200), 상기 사용자 단말(100)의 CPNS 서비스 이용이 가능하도록 인증키를 발급하는 CPNS 장치(300)를 포함한다.

[37] 상기 사용자 단말(100)은 근거리 무선 통신 기능이 탑재되어, 사용자에 의해 입력된 아이디 및 비밀번호를 포함하는 단말정보의 등록을 상기 게이트웨이(200)에 요청하여 상기 CPNS 장치(300)에 상기 단말정보가 등록되도록 한다. 상기 단말 정보는 상기 사용자에 의해 입력된 아이디와 비밀번호, 단말의 고유번호, 단말 기종, 단말 종류 등을 포함한다.

[38] 또한, 상기 사용자 단말(100)은 사용자에 의해 CPNS 서비스 이용을 위한 아이디 및 비밀번호가 입력된 경우, 상기 아이디와 비밀번호를 포함하는 단말정보를 상기 비밀번호를 이용하여 암호화하고, 상기 암호화된 단말정보를 포함하는 인증 요청 신호를 상기 게이트웨이(200)에 전송하여 상기 CPNS

장치(300)에서 생성된 인증키를 수신한다. 이때, 상기 CPNS 장치(300)로부터 수신된 인증키는 암호화된 인증키로서 상기 사용자 단말(100)은 상기 암호화된 인증키를 저장하고, 상기 수신된 인증키를 이용하여 CPNS 서비스를 이용할 수 있게 된다.

[39] 상기 사용자 단말(100)은 퍼스널 멀티미디어 플레이어(PMP), MP3 Player, 자동차 네비게이션 단말기, 휴대폰, 게임기 등과 같이 근거리 무선 통신 기능을 구비한 휴대용 단말을 의미한다.

[40] 만약, 상기 사용자 단말(100)이 이동 통신망을 통해 정보를 송수신해야 할 경우, 상기 사용자 단말(100)은 이동 통신 기능도 추가로 포함하는 것이 가능하다.

[41] 여기서, 근거리 무선 통신망은 무선랜, 블루투스, UWB(UltraWideBand), Wi-Fi 등을 비롯하여 근거리 무선 통신이 가능한 통신망을 모두 포함한다.

[42] 상기와 같은 역할을 수행하는 사용자 단말(100)에 대한 상세한 설명은 도 2를 참조하기로 한다.

[43] 상기 게이트웨이(200)는 이동 통신 기능 또는 근거리 무선 통신 기능을 탑재하여, 상기 사용자 단말(100)로부터의 단말정보 등록 요청에 따라 상기 단말정보를 저장함과 동시에 이동통신망을 통해 CPNS 장치(300)에 전송한다.

[44] 또한, 상기 게이트웨이(200)는 상기 사용자 단말(100)로부터 인증 요청 신호가 수신된 경우 상기 인증 요청 신호에 포함된 암호화된 단말정보를 상기 CPNS 장치(300)에 전송하여 인증을 요청한다.

[45] 여기에서는 상기 게이트웨이(200)와 CPNS 장치(300)를 연결하는 통신망을 이동통신망으로 한정하여 설명하였으나, 그 통신망은 이동 통신망, 근거리 무선 통신망, 유선 통신망 등을 비롯하여 모든 통신망을 의미한다.

[46] 상기 게이트웨이(200)는 유선망(예를 들어, 인터넷)을 통해 통신을 수행하는 PC(Personal Computer)와 같은 유선 단말이거나, 이동 통신망을 통해 무선인터넷을 사용할 수 있는 휴대폰, PDA 등과 같은 이동통신 단말이거나 또는 상기 유선 단말과 이동통신 단말의 기능을 모두 포함하는 단말을 의미한다.

[47] 따라서, 상기 게이트웨이(200)는 유선 단말, 무선 단말, 근거리 무선 단말 등을 말하고, 유무선 통신이 모두 가능하다.

[48] 상기 CPNS 장치(300)는 상기 게이트웨이(200)로부터 단말정보를 수신하여 저장하고, 상기 게이트웨이(200)로부터의 인증 요청에 따라 암호화된 단말정보를 해독하여 사용자 인증을 수행하고, 인증된 경우 CPNS 서비스를 위한 인증키를 생성한다.

[49] 또한, 상기 CPNS 장치(300)는 상기 인증키를 상기 비밀번호를 이용하여 암호화하고, 상기 암호화된 인증키를 상기 게이트웨이(200)를 통해 상기 사용자 단말(100)에 제공한다.

[50] 상기와 같은 역할을 수행하는 CPNS 장치(300)에 대한 상세한 설명은 도 3을 참조하기로 한다.

[51] 상기에서는 하나의 사용자 단말(100)이 단말정보의 등록을 요청하고, CPNS

서비스 이용을 위한 아이디 및 비밀번호를 입력 받아 인증키를 수신하는 기술에 대해 설명하였으나, 일단 단말정보가 CPNS 장치(300)에 등록된 이후에는 상기 아이디 및 비밀번호만을 이용하여 다른 여러 개의 단말을 이용하여 인증키를 발급받아 CPNS 서비스를 이용할 수 있다.

[52] 상기와 같은 사용자 인증을 위한 인증키 발급 기술은 클라우드 컴퓨팅 서비스 이용을 위한 사용자 인증 절차에 이용될 수 있다.

[53] 클라우드 컴퓨팅 서비스에 따르면, 사용자들은 어떠한 장소에서든 네트워크 접속과 기본적인 연산기능만을 수행하는 사용자 단말을 통해 클라우드 망에 접속하여 대용량의 저장장치와 고성능 컴퓨팅 리소스가 필요한 작업들을 수행하고, 고도화된 서비스들도 제공받을 수 있다. 이때, 사용자 단말은 클라우드 컴퓨팅 서비스 이용을 위한 클라우드 망 접속을 위해 아이디 및 비밀번호를 상기 비밀번호로 암호화하여 상기 클라우드 망에 전송하고, 상기 클라우드 망은 상기 사용자 단말에 인증키를 제공하여 상기 사용자 단말이 클라우드 컴퓨팅 서비스를 이용할 수 있도록 한다. 여기에서는 설명의 편의를 위해 클라우드 망이라고 표현하였으나, 클라우드 서버 또는 클라우드 컴퓨팅 서비스 제공을 위한 CPNS 장치로 표현 가능하다. 이때의 CPNS 장치는 여러 곳에 분산되어 있는 데이터 센터를 가상화 기술로 통합하여 사용자들이 필요로 하는 서비스를 제공하게 된다. 서비스 사용자는 어플리케이션(Application), 스토리지(Storage), 운영체제(Operation System, OS), 보안(Security)등의 필요한 컴퓨팅 자원을 각 사용자 소유의 단말에 설치하여 사용하는 것이 아니라, 가상화 기술을 통해 생성된 가상공간상의 서비스를 원하는 시점에 원하는 만큼 골라서 사용하게 된다.

[54] 도 2는 도 1에 도시된 사용자 단말의 구성을 개략적으로 나타낸 블럭도이다.

[55] 도 2를 참조하면, 사용자 단말(100)은 근거리 무선 통신망을 통해 정보를 송수신하기 위한 통신 인터페이스부(102), 사용자 명령을 입력받는 입력부(104), 출력부(106), 저장부(108), 단말정보 등록 요청부(110), 암호화부(112), 인증 요청부(114), 인증키 관리부(116), 서비스 실행부(117)를 포함한다.

[56] 상기 단말정보 등록 요청부(110)는 상기 입력부(104)를 통해 입력된 아이디 및 비밀번호를 포함하는 단말정보를 근거리 무선 통신망을 통해 상기 게이트웨이에 전송하여 상기 CPNS 장치에 등록 요청한다. 상기 단말 정보는 상기 사용자에 의해 입력된 아이디와 비밀번호, 단말의 고유번호, 단말 기종, 단말 종류 등을 포함한다.

[57] 또한, 상기 단말 정보 등록 요청부(110)는 상기 아이디 및 비밀번호를 포함하는 단말정보를 상기 비밀번호를 이용하여 암호화하고, 상기 암호화된 단말정보를 근거리 무선 통신망을 통해 상기 게이트웨이에 전송하여 상기 CPNS 장치에 등록 요청할 수도 있다.

[58] 상기 암호화부(112)는 상기 입력부(104)를 통해 CPNS 서비스 이용을 위한 아이디 및 비밀번호가 입력된 경우, 상기 아이디와 비밀번호를 포함하는

단말정보를 상기 비밀번호를 이용하여 암호화한다. 이때, 상기 암호화부(112)는 상기 아이디, 비밀번호, 단말 고유번호 등을 포함하는 단말정보를 상기 비밀번호를 이용하여 암호화할 수 있다.

[59] 상기 인증 요청부(114)는 상기 암호화부(112)에서 암호화된 단말정보를 포함하는 인증 요청 신호를 상기 통신 인터페이스부(102)를 통해 게이트웨이에 전송한다.

[60] 상기 인증키 관리부(116)는 상기 인증 요청부(114)의 인증 요청에 따라 CPNS 장치에서 생성된 인증키를 상기 게이트웨이로부터 수신하여 저장한다. 이때, 상기 게이트웨이로부터 수신된 인증키는 상기 CPNS 장치에서 생성 및 암호화된 인증키일 수 있다.

[61] 상기 서비스 실행부(117)는 상기 인증키 관리부(116)에 저장된 인증키를 이용하여 CPNS 서비스를 실행한다. 즉, 상기 서비스 실행부(117)는 상기 인증키를 통해 상기 CPNS 장치에 접속하여 CPNS 서비스를 실행하게 된다.

[62] 도 3은 도 1에 도시된 CPNS 장치의 구성을 개략적으로 나타낸 블럭도이다.

[63] 도 3을 참조하면, CPNS 장치(200)는 이동 통신망을 통해 정보를 송수신하기 위한 통신 인터페이스부(302), 단말정보 데이터베이스(306), 단말정보 등록부(304), 인증부(308), 인증키 생성부(310), 인증키 제공부(312)를 포함한다.

[64] 상기 단말정보 데이터베이스(306)에는 사용자 단말의 아이디와 비밀번호를 포함하는 단말정보와 인증키가 매핑되어 있다. 이때, 상기 단말정보에는 사용자 단말의 고유번호, 단말종류, 단말 기종 등을 포함할 수 있다.

[65] 상기 단말정보 등록부(304)는 상기 통신 인터페이스부(302)를 통해 아이디 및 비밀번호를 포함하는 단말정보의 등록이 요청된 경우, 상기 단말정보를 상기 단말정보 데이터베이스에 저장한다.

[66] 상기 인증부(308)는 상기 통신 인터페이스부(302)를 통해 게이트웨이로부터 인증 요청 신호가 수신된 경우, 상기 인증 요청 신호에 포함된 단말정보를 해독하고, 상기 해독된 단말정보가 상기 단말정보 데이터베이스(306)에 존재하는지의 여부를 이용하여 사용자 인증을 수행한다. 즉, 상기 인증부(308)는 상기 단말정보에 포함된 아이디 및 비밀번호가 상기 단말정보 데이터베이스(306)에 존재하는지의 여부를 판단한다. 상기 판단결과 상기 아이디 및 비밀번호가 상기 단말정보 데이터베이스(306)에 존재하는 경우, 상기 인증부(308)는 인증된 사용자라고 판단한다.

[67] 상기 인증키 생성부(310)는 상기 인증부(308)의 인증결과 사용자가 인증된 경우, CPNS 서비스를 위한 인증키를 생성한다.

[68] 상기 인증키 제공부(312)는 상기 생성된 인증키를 상기 비밀번호를 이용하여 암호화하고, 상기 암호화된 인증키를 상기 게이트웨이를 통해 해당 사용자 단말에 제공한다.

[69] 도 4는 본 발명의 일 실시예에 따른 CPNS 환경에서 사용자 인증을 위한 인증키 발급 방법을 나타낸 도면이다.

[70] 도 4를 참조하면, 사용자가 단말 정보의 등록을 원하여 아이디 및 비밀번호를 입력하면(S400), 사용자 단말은 상기 아이디 및 비밀번호를 포함하는 단말정보의 등록을 게이트웨이에 요청한다(S402).

[71] 상기 게이트웨이는 상기 사용자 단말로부터의 단말정보 등록 요청에 따라 상기 단말정보를 저장하고(S404), 상기 단말정보를 이동통신망을 통해 CPNS 장치에 전송한다(S406).

[72] 상기 CPNS 장치는 상기 게이트웨이로부터의 단말정보를 저장한다(S408).

[73] 추후, 사용자 단말이 상기 사용자로부터 CPNS 서비스 이용을 위한 아이디 및 비밀번호를 입력 받으면(S410), 상기 사용자 단말은 상기 아이디와 비밀번호를 포함하는 단말정보를 상기 비밀번호를 이용하여 암호화한다(S412).

[74] 그런 다음 상기 사용자 단말은 상기 암호화된 단말정보를 포함하는 인증 요청 신호를 근거리 무선 통신망을 통해 게이트웨이에 전송한다(S414).

[75] 상기 게이트웨이는 상기 인증 요청 신호내 암호화된 단말정보를 저장함과 동시에 이동통신망을 통해 CPNS 장치에 전송하여 인증을 요청한다(S416).

[76] 그러면, 상기 CPNS 장치는 상기 게이트웨이로부터의 인증 요청에 따라 상기 암호화된 단말정보를 해독하여 사용자 인증을 수행한다(S418). 즉, 상기 CPNS 장치는 상기 해독된 단말정보가 기 저장된 데이터베이스에 존재하는지의 여부를 이용하여 사용자 인증을 수행한다.

[77] 상기 인증결과 상기 사용자가 인증된 경우(S420), 상기 CPNS 장치는 CPNS 서비스를 위한 인증키를 생성하고(S422), 상기 생성된 인증키를 상기 비밀번호를 이용하여 암호화한다(S424).

[78] 그런 다음 상기 CPNS 장치는 상기 암호화된 인증키를 상기 게이트웨이를 통해 상기 사용자 단말에 제공한다(S426).

[79] 그러면, 상기 사용자 단말은 상기 인증키를 이용하여 상기 게이트웨이를 통해 상기 CPNS 장치와 접속되어 CPNS 서비스를 수행할 수 있게 된다(S428).

[80] 만약, 상기 S420의 인증결과 상기 사용자가 인증된 사용자가 아니면, 상기 CPNS 장치는 상기 사용자가 인증된 사용자가 아니라는 메시지를 상기 게이트웨이를 통해 상기 사용자 단말에 전송한다(S430).

[81] 사용자의 비밀번호를 지속적으로 key로 사용할 경우 노출의 위험이 있는바, 상기 비밀번호는 사용자 인증이 완료되고 인증키가 전달되기 전까지 “임시 credential”역할만을 하게 되며, 향후에는 상기 CPNS 장치에서 발급된 인증키가 사용된다.

[82] 도 5는 본 발명의 다른 실시예에 따른 CPNS 환경에서 사용자 인증을 위한 인증키 발급 시스템을 나타낸 도면이다.

[83] 도 5를 참조하면, CPNS 환경에서 사용자 인증을 위한 인증키 발급 시스템은 근거리 무선 통신 기능이 탑재된 사용자 단말(500), 이동통신 기능 및 근거리 무선 통신 기능이 탑재되어 상기 사용자 단말이 CPNS 서비스를 이용할 수 있도록 인증키를 발급하는 게이트웨이(600)를 포함한다.

[84] 상기 사용자 단말(500)은 사용자에 의해 입력된 아이디 및 비밀번호를 포함하는 단말정보의 등록을 게이트웨이(600)에 요청하고, CPNS 서비스 이용을 위한 아이디 및 비밀번호가 입력된 경우, 상기 아이디와 비밀번호를 포함하는 단말정보를 상기 비밀번호를 이용하여 암호화하고, 상기 암호화된 단말정보를 포함하는 인증 요청 신호를 상기 게이트웨이(600)에 전송하여 상기 게이트웨이(600)로부터 인증키를 수신한다.

[85] 상기와 같은 역할을 수행하는 사용자 단말(500)은 도 2와 상응하므로 그 상세한 설명은 생략하기로 한다.

[86] 상기 게이트웨이(600)는 상기 사용자 단말(500)로부터의 단말정보 등록 요청에 따라 상기 단말정보를 저장한다.

[87] 또한, 상기 게이트웨이(600)는 상기 사용자 단말(500)로부터 인증 요청 신호가 수신된 경우, 상기 인증 요청 신호에 포함된 암호화된 단말정보를 해독하여 사용자 인증을 수행하고, 인증된 경우 CPNS 서비스를 위한 인증키를 생성한다.

[88]

[89] 그런 다음 상기 게이트웨이(600)는 상기 비밀번호를 이용하여 상기 생성된 인증키를 암호화하고, 상기 암호화된 인증키를 상기 사용자 단말(500)에 제공한다.

[90] 또한, 상기 게이트웨이(600)는 상기 암호화된 인증키를 CPNS 장치(미도시)에 제공할 수도 있다. 그러면, 상기 사용자 단말(500)은 인증키를 통해 상기 CPNS 장치에 접속되어 CPNS 서비스를 이용할 수 있다.

[91] 상기와 같은 역할을 수행하는 게이트웨이(600)에 대한 상세한 설명은 도 6을 참조하기로 한다.

[92] 상기 사용자 단말(500)과 상기 게이트웨이(600) 간의 연결 인터페이스는 USB(Universal Serial Bus), Serial, 블루투스(Bluetooth) 등과 같은 다양한 유무선 통신이 가능한 연결 인터페이스이다.

[93] 도 6은 도 5에 도시된 게이트웨이의 구성을 개략적으로 나타낸 블럭도이다.

[94] 도 6을 참조하면, 게이트웨이(600)는 통신망을 통해 정보를 송수신하기 위한 통신 인터페이스부(602), 단말정보 데이터베이스(606), 단말정보 등록부(604), 인증부(608), 인증키 생성부(610), 인증키 제공부(612)를 포함한다.

[95] 상기 단말정보 데이터베이스(606)에는 사용자 단말의 아이디와 비밀번호를 포함하는 단말정보와 인증키가 매핑되어 있다.

[96] 상기 단말정보 등록부(604)는 상기 통신 인터페이스부(602)를 통해 아이디 및 비밀번호를 포함하는 단말정보의 등록이 요청된 경우, 상기 단말정보를 상기 단말정보 데이터베이스(606)에 저장한다. 상기 단말 정보는 상기 아이디와 비밀번호, 단말의 고유번호, 단말 기종, 단말 종류 등을 포함한다.

[97] 상기 인증부(608)는 상기 사용자 단말로부터 CPNS 서비스 이용을 위한 인증 요청 신호가 수신된 경우, 상기 인증 요청 신호에 포함된 단말정보를 해독하고, 상기 해독된 단말정보가 상기 단말정보 데이터베이스(606)에 존재하는지의

여부를 이용하여 사용자 인증을 수행한다.

[98] 상기 인증키 생성부(610)는 상기 인증부(608)의 인증결과 상기 사용자가 인증된 경우, CPNS 서비스를 위한 인증키를 생성한다.

[99] 상기 인증키 제공부(612)는 상기 생성된 인증키를 상기 비밀번호를 이용하여 암호화하고, 상기 암호화된 인증키를 상기 사용자 단말에 제공한다.

[100] 또한, 상기 인증키 제공부(612)는 상기 암호화된 인증키를 CPNS 장치(미도시)에 제공할 수도 있다.

[101] 도 7은 본 발명의 다른 실시예에 따른 CPNS 환경에서 사용자 인증을 위한 인증키 발급 방법을 나타낸 도면이다.

[102] 도 7을 참조하면, 사용자가 단말 정보의 등록을 원하여 아이디 및 비밀번호를 입력하면(S700), 사용자 단말은 상기 아이디 및 비밀번호를 포함하는 단말정보의 등록을 게이트웨이에 요청한다(S702).

[103] 상기 게이트웨이는 상기 사용자 단말로부터의 단말정보 등록 요청에 따라 상기 단말정보를 저장한다(S704). 이때, 상기 게이트웨이는 상기 단말정보를 CPNS 장치에 전송할 수도 있다.

[104] 추후, 사용자 단말이 CPNS 서비스 이용을 위한 아이디 및 비밀번호를 입력 받으면(S706), 상기 사용자 단말은 상기 아이디와 비밀번호를 포함하는 단말정보를 상기 비밀번호를 이용하여 암호화한다(S708).

[105] 그런 다음 상기 사용자 단말은 상기 암호화된 단말정보를 포함하는 인증 요청 신호를 통신망을 통해 게이트웨이에 전송한다(S710).

[106] 상기 게이트웨이는 상기 사용자 단말로부터의 인증 요청에 따라 상기 암호화된 단말정보를 해독하여 사용자 인증을 수행한다(S712). 즉, 상기 게이트웨이는 상기 해독된 단말정보가 기 저장된 데이터베이스에 존재하는지의 여부를 이용하여 사용자 인증을 수행한다.

[107] 상기 인증결과 상기 사용자가 인증된 경우(S714), 상기 게이트웨이는 CPNS 서비스를 위한 인증키를 생성하고(S716), 상기 생성된 인증키를 상기 비밀번호를 이용하여 암호화한다(S718).

[108] 그런 다음 상기 게이트웨이는 상기 암호화된 인증키를 상기 사용자 단말에 제공한다(S720). 이때, 상기 게이트웨이는 상기 암호화된 인증키를 CPNS 장치에 전송한다.

[109] 그러면, 상기 사용자 단말은 상기 인증키를 통해 상기 CPNS 장치에 접속되어 CPNS 서비스를 수행할 수 있게 된다(S722).

[110] 만약, 상기 S714의 인증결과 상기 사용자가 인증된 사용자가 아니면, 상기 게이트웨이는 상기 사용자가 인증된 사용자가 아니라는 메시지를 상기 사용자 단말에 전송한다(S724).

[111] 도 8은 본 발명의 또 다른 실시예에 따른 CPNS 환경에서 사용자 인증을 위한 인증키 발급이 가능한 사용자 단말의 구성을 개략적으로 나타낸 블럭도이다.

[112] 도 8을 참조하면, CPNS 환경에서 사용자 인증을 위한 인증키 발급이 가능한

사용자 단말(800)은 통신망을 통해 정보를 송수신하기 위한 통신 인터페이스부(802), 사용자 명령을 입력받는 입력부(804), 출력부(806), 저장부(808), 인증키 생성부(810), 인증키 제공부(812), 서비스 실행부(814)를 포함한다.

[113] 상기 인증키 생성부(810)는 상기 입력부(804)를 통해 CPNS 서비스 이용을 위한 아이디 및 비밀번호가 입력된 경우, 상기 아이디와 비밀번호를 저장함과 동시에 인증키를 생성한다.

[114] 상기 인증키 제공부(812)는 상기 아이디 및 비밀번호를 포함하는 단말정보와 상기 생성된 인증키를 상기 비밀번호를 이용하여 암호화하여 CPNS 장치로 전송한다.

[115] 그러면, 상기 CPNS 장치는 기 저장된 단말정보 데이터베이스에서 상기 단말정보를 검색하고, 그 단말정보에 상기 인증키를 매핑하여 저장한다. 그런 다음 상기 CPNS 장치는 상기 인증키를 통해 상기 사용자 단말이 접속되어 CPNS 서비스를 제공받도록 한다.

[116] 상기 서비스 실행부(814)는 상기 인증키 생성부(810)에서 생성된 인증키를 이용하여 CPNS 서비스를 실행한다.

[117] 도 9는 도 8에 도시된 사용자 단말이 CPNS 환경에서 사용자 인증을 위한 인증키를 발급하는 방법을 나타낸 흐름도이다.

[118] 도 9를 참조하면, 사용자 단말은 사용자에 의해 CPNS 서비스 이용을 위한 아이디 및 비밀번호를 입력받으면(S900), 상기 아이디와 비밀번호를 저장함과 동시에 인증키를 생성한다(S902).

[119] 그런 다음 상기 사용자 단말은 상기 아이디 및 비밀번호를 포함하는 단말정보와 상기 생성된 인증키를 상기 비밀번호를 이용하여 암호화하여 CPNS 장치로 전송한다(S904). 즉, 상기 사용자 단말은 상기 CPNS 장치에 아이디 및 비밀번호를 포함하는 단말정보, 인증키 등을 제공하여, 추후 상기 사용자가 다른 단말을 이용하여 CPNS 서비스를 이용할 수 있도록 한다.

[120] 상기 사용자 단말은 상기 인증키를 이용하여 CPNS 서비스를 실행한다(S906).

[121] 이와 같이, 본 발명이 속하는 기술분야의 당업자는 본 발명이 그 기술적 사상이나 필수적 특징을 변경하지 않고서 다른 구체적인 형태로 실시될 수 있다는 것을 이해할 수 있을 것이다. 그러므로 이상에서 기술한 실시예들은 모든 면에서 예시적인 것이며 한정적인 것이 아닌 것으로서 이해해야만 한다. 본 발명의 범위는 상기 상세한 설명보다는 후술하는 특허청구범위에 의하여 나타내어지며, 특허청구범위의 의미 및 범위 그리고 그 등가개념으로부터 도출되는 모든 변경 또는 변형된 형태가 본 발명의 범위에 포함되는 것으로 해석되어야 한다.

[122]

[123] <부호의 설명>

[124] 100, 500, 800 : 사용자 단말 102, 302, 602 : 통신 인터페이스부

[125] 104, 804 : 입력부 106, 806 : 출력부

[126] 108, 808 : 저장부 110 : 단말정보 등록 요청부

[127] 112 : 암호화부 114 : 인증 요청부

[128] 116 : 인증키 관리부 117 : 서비스 실행부

[129] 200, 600 : 게이트웨이 300 CPNS 장치

[130] 304, 604 : 단말 정보 등록부 306, 606 : 단말정보 데이터베이스

[131] 308, 608 : 인증부 310, 610, 810 : 인증키 생성부

[132] 312, 612, 812 : 인증키 제공부 814 : 서비스 실행부

청구범위

[청구항 1] 근거리 무선 통신 기능이 탑재되어, 아이디(ID) 및 비밀번호를 포함하는 단말정보의 등록을 게이트웨이에 요청하고, CPNS(Converged Personal Network Service) 서비스 이용을 위한 아이디 및 비밀번호가 입력된 경우, 상기 아이디 및 비밀번호를 포함하는 단말정보를 상기 비밀번호를 이용하여 암호화하고, 상기 암호화된 단말정보를 포함하는 인증 요청 신호를 상기 게이트웨이에 전송하여 CPNS 장치에서 생성된 인증키를 수신하는 사용자 단말;
이동 통신 기능 또는 근거리 무선 통신 기능을 탑재하여, 상기 사용자 단말로부터의 단말정보 등록 요청에 따라 상기 단말정보를 이동통신망을 통해 CPNS 장치에 전송하고, 상기 사용자 단말로부터 인증 요청 신호가 수신된 경우 상기 암호화된 단말정보를 상기 CPNS 장치에 전송하여 인증을 요청하는 게이트웨이; 및
상기 게이트웨이로부터의 단말정보를 저장하고, 상기 게이트웨이로부터의 인증 요청에 따라 상기 암호화된 단말정보를 해독하여 사용자 인증을 수행하고, 인증된 경우 CPNS 서비스를 위한 인증키를 생성하고, 상기 생성된 인증키를 상기 비밀번호를 이용하여 암호화한 후, 상기 게이트웨이를 통해 상기 사용자 단말에 제공하는 CPNS 장치;
를 포함하는 CPNS 환경에서 사용자 인증을 위한 인증키 발급 시스템.

[청구항 2] 제1항에 있어서,
상기 게이트웨이는 상기 사용자 단말로부터의 단말정보 등록 요청에 따라 단말정보를 저장한 후, 상기 사용자 단말로부터 인증 요청 신호가 수신된 경우 상기 암호화된 단말정보를 해독하여 사용자 인증을 수행하고, 인증된 경우 CPNS 서비스를 위한 인증키를 생성하고, 상기 생성된 인증키를 상기 비밀번호를 이용하여 암호화한 후 상기 사용자 단말 및 CPNS 장치에 제공하는 것을 특징으로 하는 CPNS 환경에서 사용자 인증을 위한 인증키 발급 시스템.

[청구항 3] 통신망을 통해 정보를 송수신하기 위한 통신 인터페이스부;
사용자 명령을 입력받는 입력부;
상기 입력부를 통해 CPNS 서비스 이용을 위한 아이디 및 비밀번호가 입력된 경우, 상기 아이디 및 비밀번호를 포함하는 단말정보를 상기 비밀번호를 이용하여 암호화하는 암호화부;

상기 암호화된 단말정보를 포함하는 인증 요청 신호를 상기 통신 인터페이스부를 통해 게이트웨이에 전송하는 인증 요청부; 및
상기 인증 요청에 따라 CPNS 장치에서 생성된 인증키를 상기 게이트웨이로부터 수신 및 저장하는 인증키 관리부;
를 포함하는 사용자 단말.

[청구항 4] 제3항에 있어서,
상기 입력부를 통해 입력된 아이디 및 비밀번호를 포함하는 단말정보를 근거리 무선 통신망을 통해 상기 게이트웨이에 전송하여 상기 CPNS 장치에 등록 요청하는 단말 정보 등록 요청부를 더 포함하는 사용자 단말.

[청구항 5] 제4항에 있어서,
상기 단말 정보 등록 요청부는 상기 아이디 및 비밀번호를 포함하는 단말정보를 상기 비밀번호를 이용하여 암호화하고, 상기 암호화된 단말정보를 근거리 무선 통신망을 통해 상기 게이트웨이에 전송하여 상기 CPNS 장치에 등록 요청하는 것을 특징으로 하는 사용자 단말.

[청구항 6] 제3항에 있어서,
상기 인증키를 이용하여 CPNS 서비스를 실행하는 서비스 실행부를 더 포함하는 사용자 단말.

[청구항 7] 제3항에 있어서,
상기 입력부를 통해 CPNS 서비스 이용을 위한 아이디 및 비밀번호가 입력된 경우, 상기 아이디와 비밀번호를 저장함과 동시에 인증키를 생성하는 인증키 생성부; 및
상기 아이디 및 비밀번호를 포함하는 단말정보와 상기 생성된 인증키를 상기 비밀번호를 이용하여 암호화하여 CPNS 장치로 전송하는 인증키 제공부를 더 포함하는 사용자 단말.

[청구항 8] 통신망을 통해 정보를 송수신하기 위한 통신 인터페이스부;
사용자 단말별 아이디 및 비밀번호를 포함하는 단말정보, 인증키가 저장된 단말 정보 데이터베이스;
상기 통신 인터페이스부를 통해 단말정보의 등록이 요청된 경우, 상기 단말정보를 상기 단말정보 데이터베이스에 등록하는 단말정보 등록부;
상기 통신 인터페이스부를 통해 인증 요청 신호가 수신된 경우, 상기 인증 요청 신호에 포함된 단말정보를 해독하고, 상기 해독된 단말정보가 상기 단말정보 데이터베이스에 존재하는지의 여부를 이용하여 사용자 인증을 수행하는 인증부;
상기 사용자가 인증된 경우, CPNS 서비스를 위한 인증키를 생성하는 인증키 생성부; 및

상기 생성된 인증키를 상기 단말정보에 포함된 비밀번호를 이용하여 암호화하고, 상기 암호화된 인증키를 상기 통신 인터페이스부를 통해 해당 사용자 단말에 제공하는 인증키 제공부;
를 포함하는 CPNS 장치.

[청구항 9] 제8항에 있어서,
상기 단말정보는 아이디, 비밀번호, 단말 고유번호, 단말 종류, 단말 기종 중 적어도 하나를 포함하는 것을 특징으로 하는 CPNS 장치.

[청구항 10] (a) 사용자 단말이 상기 암호화된 단말정보를 포함하는 인증 요청 신호를 근거리 무선 통신망을 통해 게이트웨이에 전송하는 단계;
(b) 상기 게이트웨이가 상기 인증 요청 신호내 암호화된 단말정보를 저장함과 동시에 이동통신망을 통해 CPNS 장치에 전송하여 인증을 요청하는 단계;
(c) 상기 CPNS 장치가 상기 게이트웨이로부터의 인증 요청에 따라 상기 암호화된 단말정보를 해독하여 사용자 인증을 수행하는 단계;
(d) 상기 사용자가 인증된 경우, 상기 CPNS 장치가 CPNS 서비스를 위한 인증키를 생성하는 단계; 및
(e) 상기 CPNS 장치가 상기 생성된 인증키를 상기 비밀번호를 이용하여 암호화하고, 상기 암호화된 인증키를 상기 게이트웨이를 통해 상기 사용자 단말에 제공하는 단계;
를 포함하는 CPNS 환경에서 사용자 인증을 위한 인증키 발급 방법.

[청구항 11] 사용자 단말이 CPNS 환경에서 사용자 인증을 위한 인증키를 발급받기 위한 방법에 있어서,
(a) 사용자에 의해 CPNS 서비스 이용을 위한 아이디 및 비밀번호가 입력된 경우, 상기 아이디와 비밀번호를 포함하는 단말정보를 상기 비밀번호를 이용하여 암호화하는 단계;
(b) 상기 암호화된 단말정보를 포함하는 인증 요청 신호를 게이트웨이에 전송하는 단계;
(c) 상기 인증 요청에 따라 CPNS 장치에서 생성된 인증키를 상기 게이트웨이로부터 수신 및 저장하는 단계; 및
(d) 상기 인증키를 통해 상기 CPNS 장치에 접속되어 CPNS 서비스를 실행하는 단계;
를 포함하는 CPNS 환경에서 사용자 인증을 위한 인증키 발급 방법.

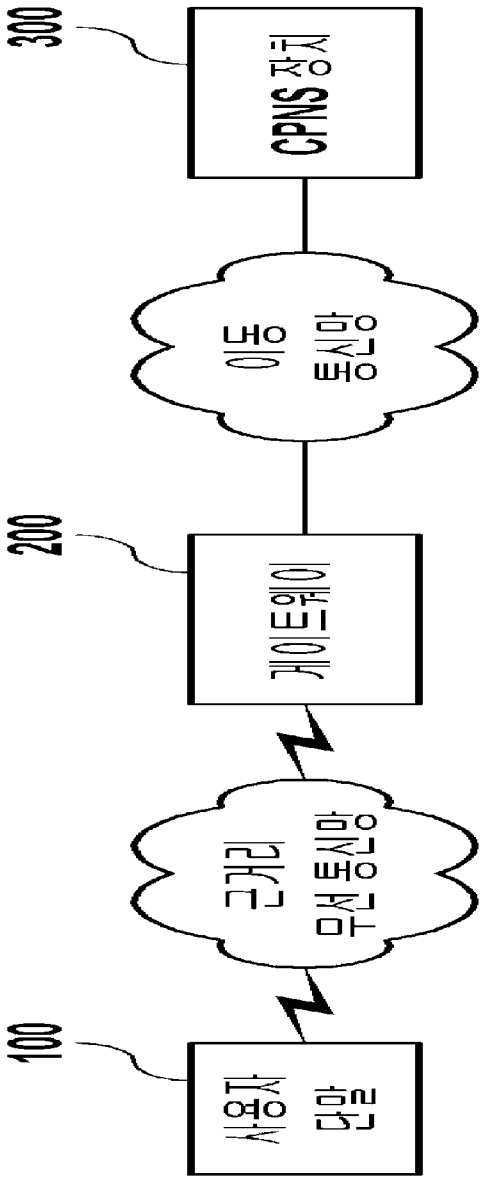
[청구항 12] 제11항에 있어서,

상기 (a) 단계 이전에,
상기 사용자에 의해 입력된 아이디 및 비밀번호를 포함하는 단말정보의 등록을 상기 게이트웨이에 요청하는 단계를 더 포함하는 CPNS 환경에서 사용자 인증을 위한 인증키 발급 방법.

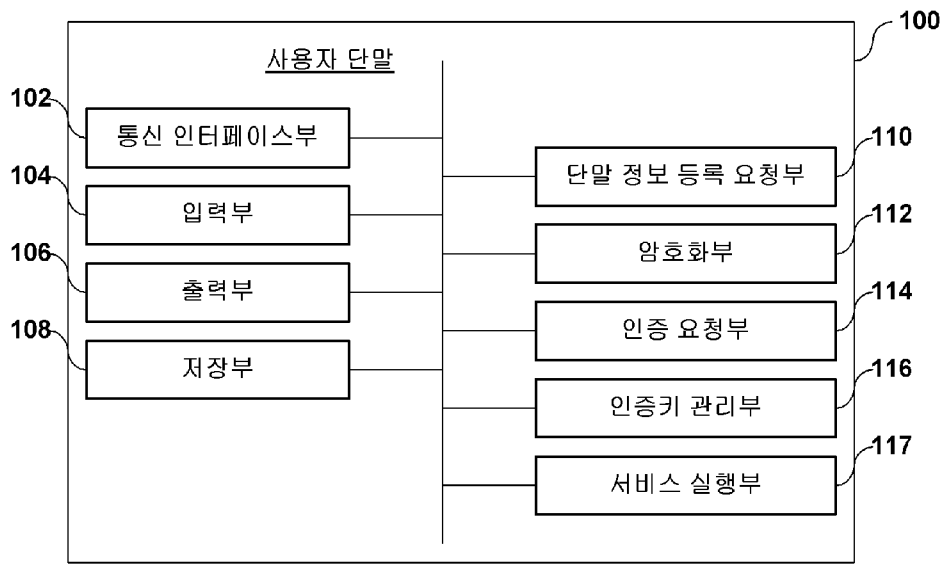
[청구항 13] CPNS 장치가 CPNS 환경에서 사용자 인증을 위한 인증키를 발급하는 방법에 있어서,
(a) CPNS 서비스 이용을 위한 인증 요청 신호가 수신된 경우, 상기 인증 요청 신호에 포함된 암호화된 단말정보를 해독하는 단계;
(b) 상기 해독된 단말정보가 기 저장된 단말정보 데이터베이스에 존재하는지의 여부를 판단하는 단계;
(c) 상기 단말정보가 상기 단말정보 데이터베이스에 존재하는 경우, CPNS 서비스를 위한 인증키를 생성하는 단계;
(d) 상기 생성된 인증키를 상기 단말정보에 포함된 비밀번호를 이용하여 암호화하는 단계; 및
(e) 상기 암호화된 인증키를 해당 사용자 단말에 제공하는 단계;
를 포함하는 CPNS 환경에서 사용자 인증을 위한 인증키 발급 방법.

[청구항 14] 제13항에 있어서,
상기 (a) 단계 이전에,
상기 사용자 단말로부터 아이디 및 비밀번호를 포함하는 단말정보의 등록이 요청된 경우, 상기 단말정보를 등록하는 단계를 더 포함하는 CPNS 환경에서 사용자 인증을 위한 인증키 발급 방법.

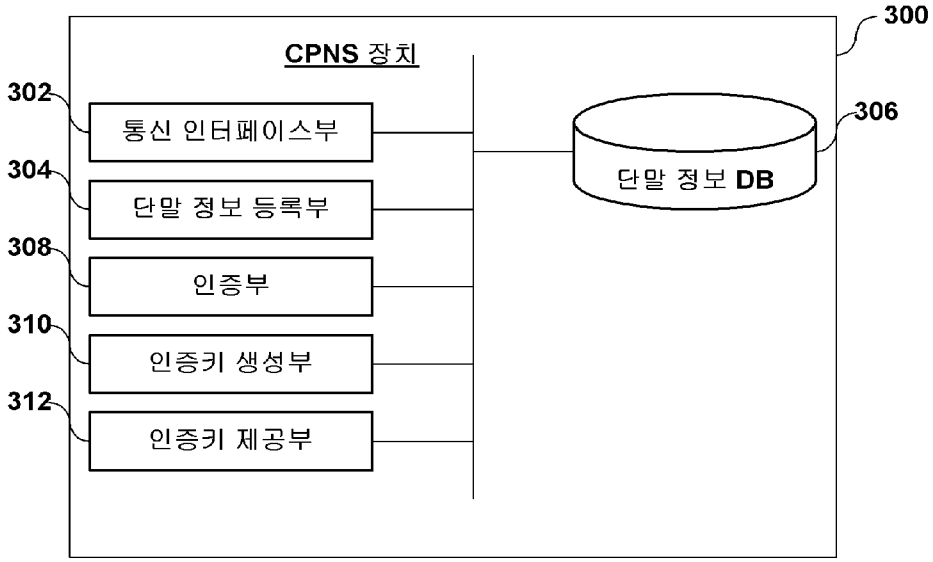
[Fig. 1]


300
CPNS 장치
인터넷 통신망
200
게이트웨이
그 외 무선 통신망
100
사용자 단말

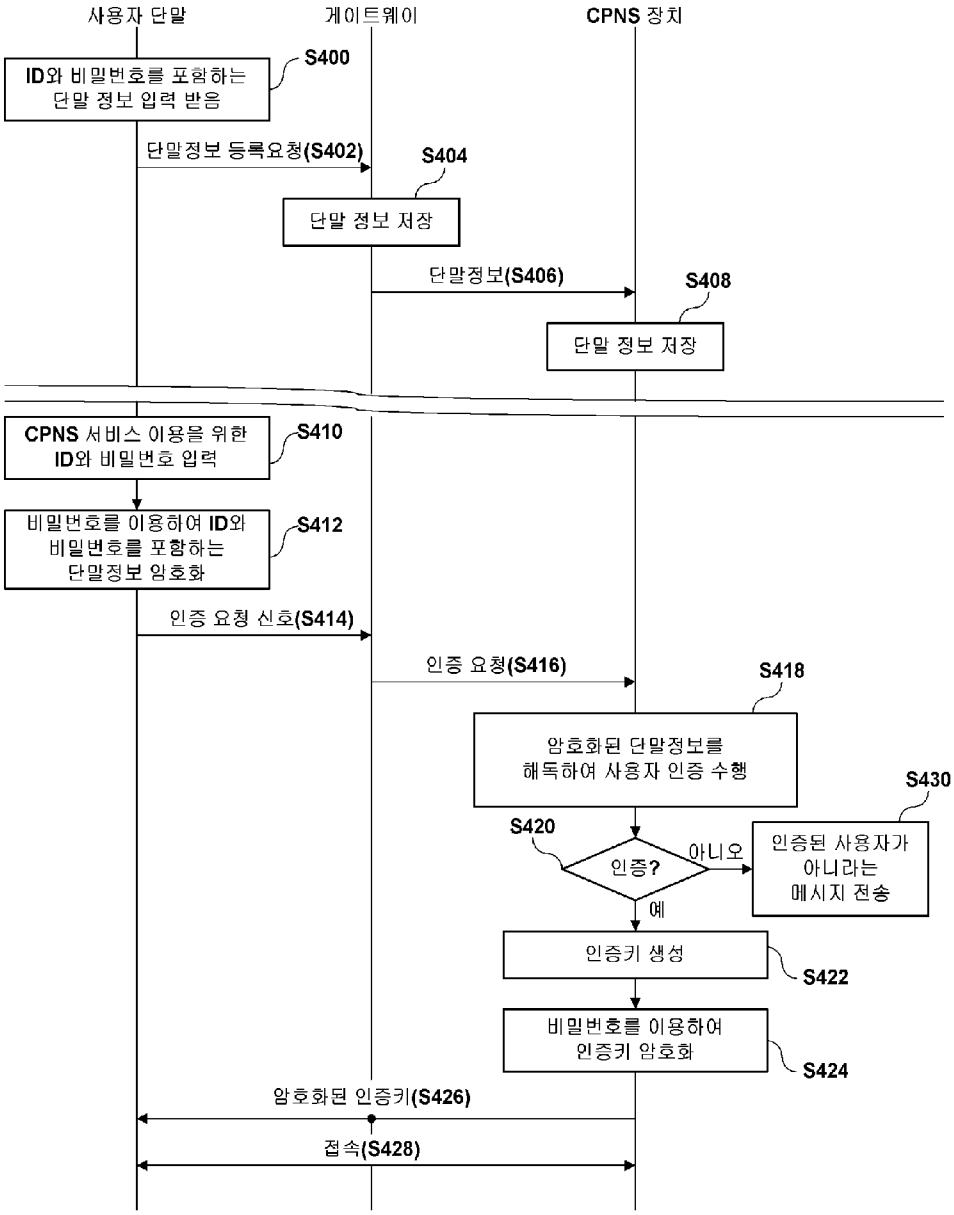
[Fig. 2]


100
사용자 단말
102
통신 인터페이스부
104
입력부
106
출력부
108
저장부
110
단말 정보 등록 요청부
112
암호화부
114
인증 요청부
116
인증키 관리부
117
서비스 실행부

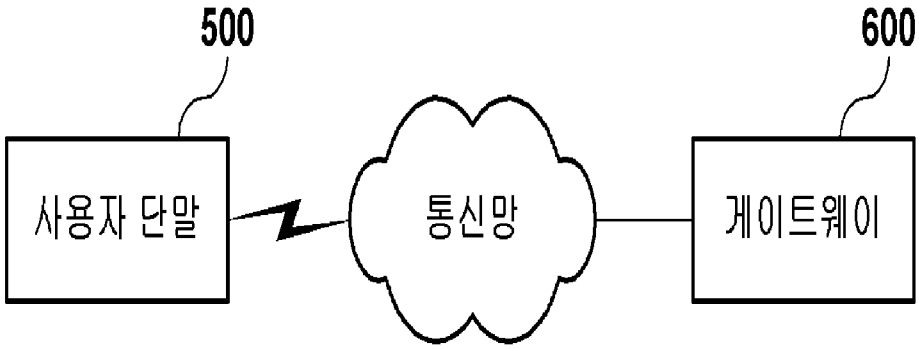
[Fig. 3]


300
CPNS 장치
302
통신 인터페이스부
304
단말 정보 등록부
308
인증부
310
인증키 생성부
312
인증키 제공부
306
단말 정보 DB

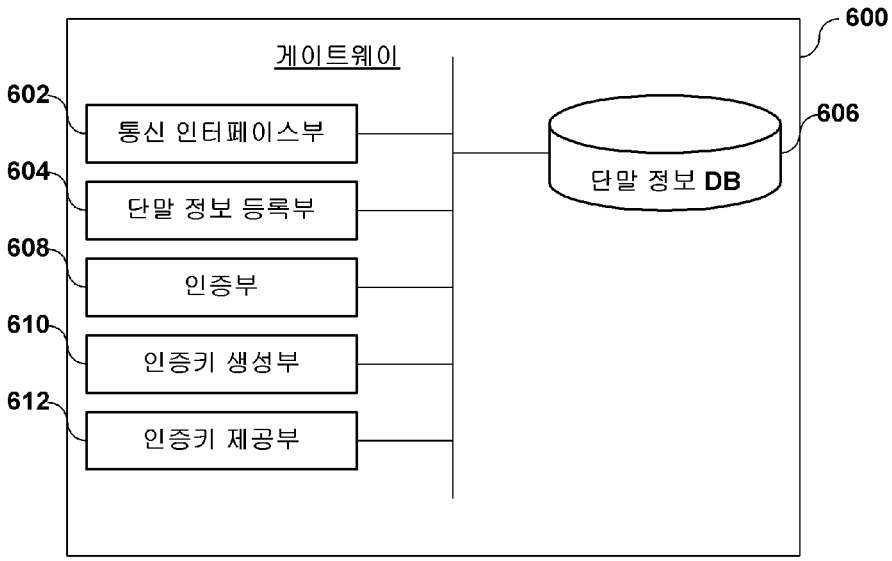
[Fig. 4]


사용자 단말
게이트웨이
CPNS 장치
ID와 비밀번호를 포함하는 단말 정보 입력 받음
S400
단말정보 등록요청(S402)
S404
단말 정보 저장
단말정보(S406)
S408
단말 정보 저장
CPNS 서비스 이용을 위한 ID와 비밀번호 입력
S410
비밀번호를 이용하여 ID와 비밀번호를 포함하는 단말정보 암호화
S412
인증 요청 신호(S414)
인증 요청(S416)
S418
암호화된 단말정보를 해독하여 사용자 인증 수행
S420
인증?
아니오
S430
인증된 사용자가 아니라는 메시지 전송
예
인증키 생성
S422
비밀번호를 이용하여 인증키 암호화
S424
암호화된 인증키(S426)
접속(S428)

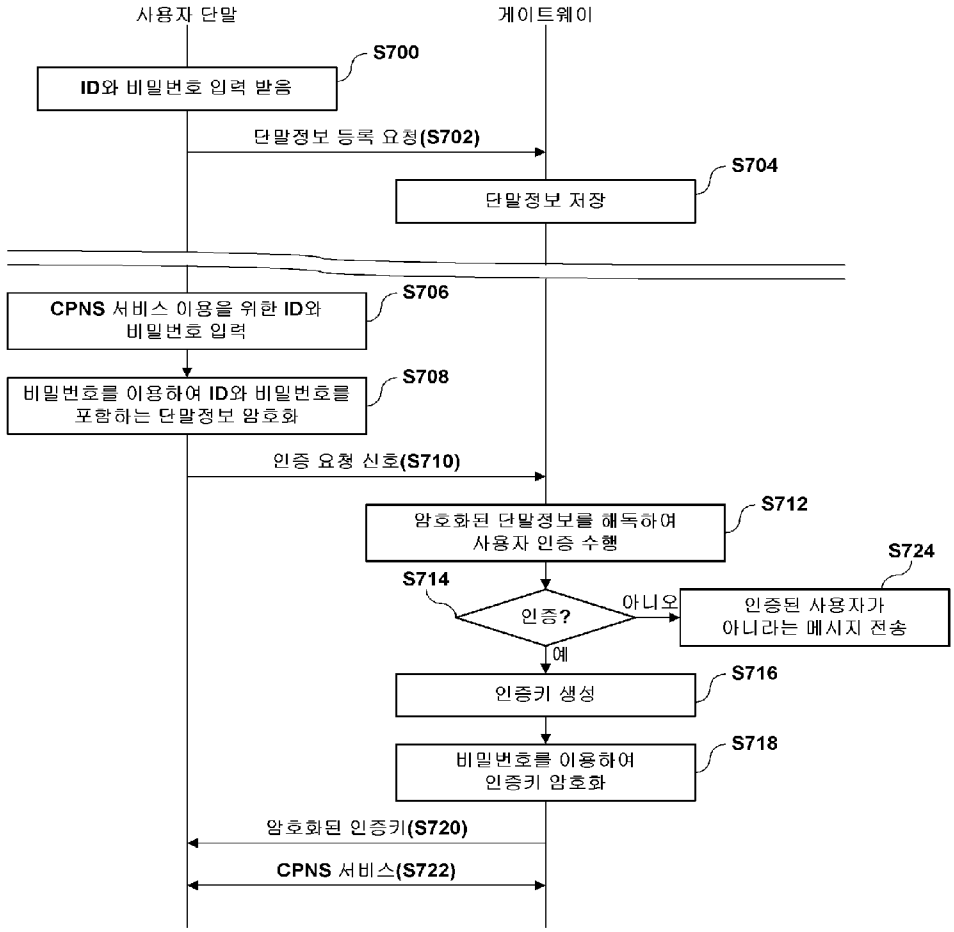
[Fig. 5]


500
600
사용자 단말
통신망
게이트웨이

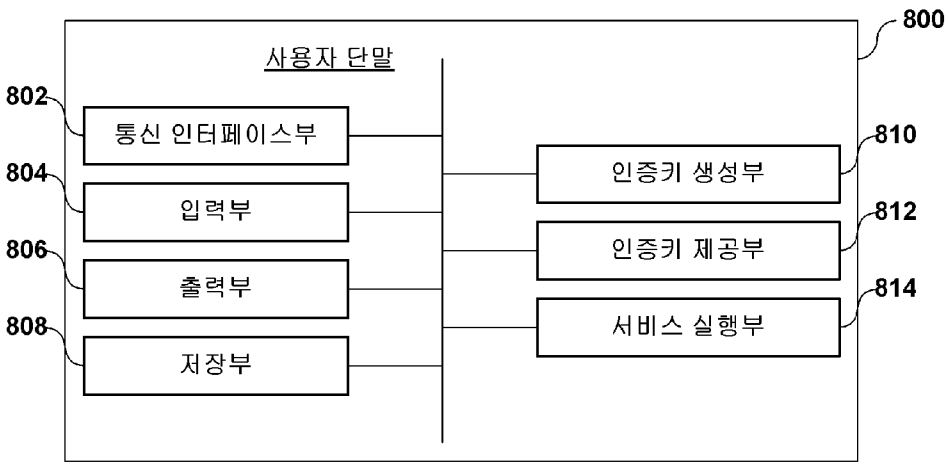
[Fig. 6]


600
게이트웨이
602
통신 인터페이스부
604
단말 정보 등록부
608
인증부
610
인증키 생성부
612
인증키 제공부
606
단말 정보 DB

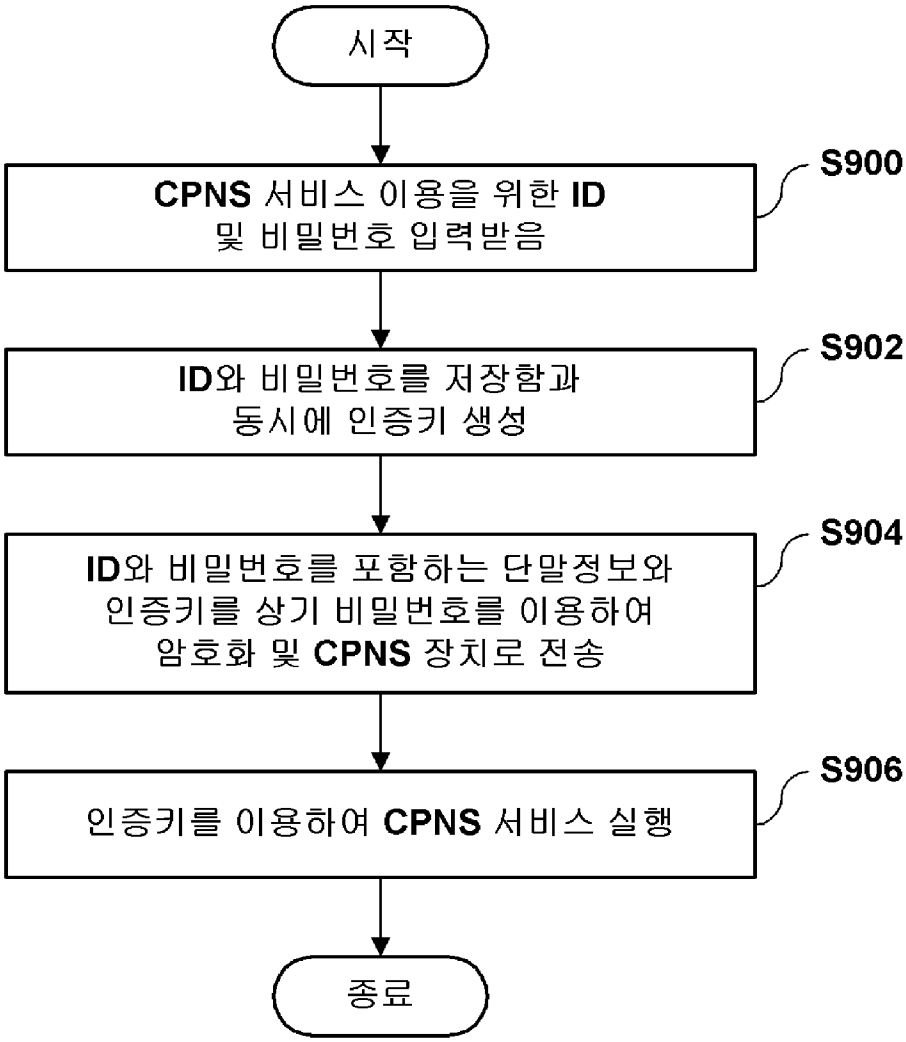
[Fig. 7]


사용자 단말
게이트웨이
S700
ID와 비밀번호 입력 받음
단말정보 등록 요청(S702)
S704
단말정보 저장
S706
CPNS 서비스 이용을 위한 ID와 비밀번호 입력
S708
비밀번호를 이용하여 ID와 비밀번호를 포함하는 단말정보 암호화
인증 요청 신호(S710)
S712
암호화된 단말정보를 해독하여 사용자 인증 수행
S724
S714
인증?
아니오
인증된 사용자가 아니라는 메시지 전송
예
S716
인증키 생성
S718
비밀번호를 이용하여 인증키 암호화
암호화된 인증키(S720)
CPNS 서비스(S722)

[Fig. 8]


800
사용자 단말
802
통신 인터페이스부
804
입력부
806
출력부
808
저장부
810
인증키 생성부
812
인증키 제공부
814
서비스 실행부

[Fig. 9]


시작
CPNS 서비스 이용을 위한 ID 및 비밀번호 입력받음
S900
ID와 비밀번호를 저장함과 동시에 인증키 생성
S902
ID와 비밀번호를 포함하는 단말정보와 인증키를 상기 비밀번호를 이용하여 암호화 및 CPNS 장치로 전송
S904
인증키를 이용하여 CPNS 서비스 실행
S906
종료